

	Sistemas de gestión de la seguridad de la información	Rev. 1
	A 5.3 – SEGREGACIÓN DE FUNCIONES	Aprobada: 01.05.2024
	Crea: COF Aprueba: CEO	Página 1 de 2

Objetivo:

Minimizar el riesgo de errores y fraudes mediante la separación adecuada de responsabilidades y funciones críticas dentro de la organización, garantizando que ninguna persona tenga el control total sobre procesos sensibles que puedan afectar la seguridad de la información.

Declaración:

La organización ha implementado controles que aseguran la segregación de funciones en actividades y procesos relacionados con la seguridad de la información, promoviendo un ambiente de control que reduce la posibilidad de actos indebidos o errores no detectados.

Alcance:

Aplica a todos los procesos, sistemas y personal que intervienen en la gestión, acceso, procesamiento y control de activos de información críticos o sensibles.

Directrices:

- Se identifican y documentan funciones y actividades críticas que requieren segregación para evitar conflictos de interés y fraudes.
- Se asignan roles y responsabilidades de forma que las tareas clave, como autorización, ejecución, registro y revisión, estén divididas entre diferentes personas.
- Se establecen procedimientos para controlar y supervisar excepciones donde la segregación no sea posible, incluyendo autorizaciones específicas y monitoreo reforzado.
- La segregación de funciones está reflejada en los perfiles de acceso y roles dentro de los sistemas de información.
- Se revisan periódicamente los controles para asegurar la efectividad de la segregación y realizar ajustes ante cambios organizacionales o tecnológicos.

Referencias relacionadas:

- POL 007 — Política de roles y responsabilidades
- PRO 014 — Procedimiento para el Registro y Supervisión de Accesos
- DOC 012 — Listado actualizado de usuario con roles
- FOR 029 — Registro de acceso área restringida - Mes actual
- PSC 007 — Monitoreo y Medición

Evidencias de implementación:

- Documentación formal que identifica funciones críticas y su segregación.

- Registros y reportes de accesos segregados y monitoreados (FOR 029).
- Listados actualizados de usuarios con roles y permisos definidos (DOC 012).
- Informes periódicos de supervisión y auditoría interna que verifican el cumplimiento de la segregación.
- Procedimientos documentados que detallan el manejo de excepciones y autorizaciones.

Historial de Versiones

Versión	Fecha	Asiento	Aprueba
001	01.02.2024	Original	CEO